

# BAB I

## PENDAHULUAN

### 1.1 Pengenalan Masalah

Dalam era digital saat ini, keamanan menjadi aspek yang sangat penting, terutama di lingkungan kos-kosan yang sering menjadi target kejahatan. Banyak penghuni kos menyimpan barang berharga, seperti elektronik dan dokumen penting, sehingga menjadikannya sasaran empuk bagi pelaku kejahatan. Pemilik kos bertanggung jawab untuk menyediakan sistem keamanan yang lebih baik, seperti pemantauan penguncian setiap kamar, serta mengawasi lingkungan dari individu dengan motif kejahatan. Pencegahan dan tindakan terjadinya kriminalitas berupa pembobolan menjadi tantangan utama dalam permasalahan ini.

Pembobolan pintu merupakan aktivitas pembukaan paksa yang dilakukan dengan merusak mekanisme penguncian atau membuka pintu tanpa melalui prosedur yang semestinya. Tindakan ini dapat dilakukan dengan berbagai cara, seperti mencongkel, mendorong paksa, atau menggunakan alat khusus untuk melewati sistem keamanan. Dalam beberapa kasus, pelaku memanfaatkan celah atau kelemahan pada penguncian tanpa harus merusaknya secara fisik.

Diperlukan solusi yang fleksibel dalam posisi dan penggunaannya, tetapi tetap memberikan dampak signifikan dibandingkan sistem keamanan yang ada di pasaran. Solusi yang tersedia saat ini, seperti kamera pemantau (CCTV) dan penguncian menggunakan RFID, belum sepenuhnya menyelesaikan masalah kriminalitas pencurian. Pencegahan yang tidak dilakukan secara proaktif dan tindakan yang cenderung terlambat dieksekusi menjadi tantangan utama dalam meningkatkan keamanan di kos-kosan.

Penggunaan peringatan suara sebagai pencegah kemalingan menjadi salah satu strategi yang efektif dalam meningkatkan keamanan di lingkungan kos-kosan. Dengan mengintegrasikan sistem peringatan suara, penghuni disekitar dapat

merespons situasi mengancam secara cepat dan memberikan intimidasi kepada pelaku kejahatan. Suara peringatan yang keras dan jelas dapat menarik perhatian, baik dari penghuni lain maupun dari masyarakat sekitar, sehingga dapat mengurangi niat jahat para maling. Selain itu, sistem ini dapat berfungsi sebagai pengingat bagi penghuni untuk tetap waspada terhadap potensi ancaman. Implementasi peringatan suara dalam sistem keamanan tidak hanya meningkatkan rasa aman, tetapi juga menciptakan lingkungan yang lebih responsif terhadap tindakan kriminal, sehingga diharapkan dapat menurunkan angka kemalingan secara signifikan.

### **1.1.1. Informasi Pendukung Masalah**

Pada tahun 2021 kejadian terhadap hak milik barang tanpa kekerasan yang dilaporkan kepada polisi (69.347 kejadian). Namun, pada tahun 2022 adanya lonjakan kasus yang cukup tajam menjadi sebanyak 91.892 kejadian dan menjadi jumlah terbesar dalam kurun waktu lima tahun terakhir tidak dilaporkan secara langsung atau masuk dalam kategori pencurian biasa yang tersebar di laporan kriminalitas nasional[1].

Pada tahun 2023, pada lokasi kos lama penulis, telah terjadi musibah pencurian. Korban kehilangan laptop saat sedang keluar kamar dan lupa mengunci pintu. Pencuri memanfaatkan kesempatan ketika korban meninggalkan kamar dalam keadaan tidak terkunci, sehingga pencurian pun terjadi. Musibah ini baru disadari setelah korban kembali dan mengetahui barangnya hilang, sementara pintu kamar masih dalam keadaan terbuka.

Kemalingan yang terjadi di kos-kosan dapat disebabkan oleh berbagai faktor yang membuat sistem keamanan menjadi rentan. Salah satu faktor utama adalah minimnya pengamanan di banyak kos-kosan, di mana fasilitas seperti kamera CCTV dan penguncian otomatis belum banyak diterapkan. Kelalaian penghuni juga menjadi penyebab signifikan, terutama ketika mereka lupa atau sengaja tidak mengunci pintu saat bepergian, sehingga memberikan peluang bagi pelaku kejahatan. Beberapa solusi

yang telah ada sampai saat ini adalah Penggunaan teknologi seperti penggunaan RFID, menggunakan pengamanan tambahan dari penggunaan *closed circuit television* (CCTV).

1. Kontrol Akses Berbasis Kartu atau RFID: Beberapa kos sudah menggunakan sistem kartu akses atau RFID yang lebih aman dibandingkan dengan kunci fisik. Sistem ini memastikan bahwa hanya penghuni yang memiliki kartu akses yang bisa membuka pintu. Salah satu penelitian terkait penggunaan RFID ini dilakukan oleh mahasiswa Universitas Muhammadiyah Malang yaitu Penelitian terhadap perancangan pintu otomatis berbasis Arduino RFID dan *Voice Recognition* Arduino. Arduino berperan sebagai otak sistem yang menerima informasi dari pembaca RFID untuk mengidentifikasi kartu yang valid, dan juga mampu memproses perintah suara yang terverifikasi melalui modul pengenalan suara. Hal ini memungkinkan pintu untuk terbuka secara otomatis ketika kartu yang terdaftar dideteksi atau perintah suara yang benar diucapkan.[2]
2. CCTV dan Sistem Pemantauan *Real-Time*: Penggunaan CCTV berbasis *cloud* memungkinkan penghuni dan pengelola untuk memantau pintu dan area sekitar kos secara *real-time* melalui aplikasi atau *platform* web. Kamera ini biasanya terhubung ke internet dan bisa mengirim notifikasi jika mendeteksi gerakan di area yang dipantau.
3. Sistem Penguncian Pintar (*Smart Locks*) berbasis IoT: Sistem kunci pintar memungkinkan pengguna untuk mengontrol kunci pintu dari jarak jauh menggunakan aplikasi Android. Ini menghilangkan kebutuhan akan kunci fisik dan memungkinkan pengguna untuk memantau status pintu, apakah terkunci atau tidak, melalui *smartphone* mereka.[3]

### **1.1.2. Analisis Masalah**

#### **1. Aspek Ekonomi**

Penghuni tidak perlu khawatir lagi tentang membeli kunci cadangan atau mengganti kunci manual yang rusak, sehingga mengurangi pengeluaran kecil tetapi berulang. Penerapan sistem keamanan berbasis teknologi dapat meningkatkan nilai jual atau nilai sewa kos, karena kos yang aman memiliki daya tarik lebih bagi calon penghuni.

#### **2. Aspek Hukum**

Sistem yang lebih aman dapat mengurangi beban dari tanggung jawab pemilik atas kehilangan barang milik penghuni. Hal ini juga dapat dikaitkan dengan peraturan perlindungan konsumen.

#### **3. Aspek Sosial**

Hal ini dapat mengurangi kecemasan penghuni, meningkatkan kenyamanan tinggal, dan meningkatkan hubungan antara penghuni dan pemilik kos. mendukung hal ini membuat peningkatan kepercayaan antar konsumen pengguna kos dan pengelola yang menangani manajemen keamanan kos.

### **1.1.3. Kebutuhan yang harus dipenuhi**

1. Alat dapat melakukan sistem automasi pembukaan dan penguncian pintu dengan constraint waktu dibawah 1 detik.
2. Dapat mendeteksi pergerakan sekitar dalam radius dibawah 2 meter.
3. Identifikasi penghuni, pihak tidak diketahui dan tingkat ancaman di sekitar kos (mengklasifikasikan identitas).
4. Alat dapat memberikan tindakan respon berupa suara pada rentang 60-80 dB (rentang suara sedang hingga keras).

#### 1.1.4. Tujuan

Membuat sebuah sistem pada pengelolaan kos yang menyelesaikan permasalahan dengan mengklasifikasi pemilik kos dan menjaga agar pintu tetap terkunci apabila tidak ada penghuni di sekitar kamar dalam pencegahan kejahatan dalam tindakan pembobolan pintu.

### 1.2 Solusi

#### 1.2.1. Karakteristik Produk

##### 1. Fitur Dasar

- a. *Computing Performance*: Pada sistem yang akan dibuat ini diperlukan kinerja alat memberikan respon secara waktu-nyata dan akurat.
- b. Otomatisasi Pembukaan dan Penguncian: fitur utama dari produk yang akan dibuat adalah dapat melakukan otomatisasi penguncian pintu ketika ada faktor yang memicu, seperti penghuni yang meninggalkan kosnya dan pembukaan ketika penghuni kembali.
- c. Notifikasi Pengguna: dapat memberi tahu pesan terkait perilaku aktivitas sistem secara real-time
- d. Metode Komputasi: Metode komputasi merupakan sebuah otak dari system yang buat. Data yang telah dikumpulkan oleh sensor atau masukan yang lain akan diproses melalui algoritma untuk mengidentifikasi masalah.
- e. Deteksi Pergerakan: fitur ini dapat menentukan pergerakan normal atau mengancam yang terjadi di sekitar pintu, baik tindakan penghuni maupun pergerakan tidak diizinkan, serta memberikan output dari keputusan tersebut.
- f. Peringatan Suara atau Sirine: menambahkan sirine atau alarm sebagai peringatan tambahan saat mendeteksi adanya aktivitas tidak diizinkan di sekitar pintu. Fitur ini berfungsi sebagai pencegah tambahan terhadap tindakan kriminal.

## 2. Fitur Tambahan

- a. *Low Power Consumption* Sistem memiliki penggunaan daya yang rendah, tidak melebihi 50 Volt
- b. *Low Cost*, Sistem dapat diselesaikan dengan biaya yang tidak lebih dari Rp 3.000.000
- c. Pencatatan aktivitas pintu, yaitu bagaimana status dari pintu atau lingkungan disekitar pintu dapat di simpan
- d. Waktu pengerjaan < 6 bulan, Proses perancangan hingga pengembangan sistem harus dapat diselesaikan dalam waktu kurang dari 6 bulan

### 1.2.2. Usulan Solusi

#### 1. Solusi 1

“Sistem Kunci Pintar Menggunakan Teknik *Geofencing* Sebagai kontrol Penguncian”

*Geo-fencing* adalah teknologi inovatif yang memanfaatkan Sistem Penentuan Posisi Global (GPS) untuk membuat batasan virtual, yang memungkinkan berbagai aplikasi seperti pengumpulan tol elektronik, iklan kontekstual, dan sistem informasi wisata.[4].

Pencegahan kemalingan yang pertama adalah dengan menerapkan automasi penguncian menggunakan algoritma *geofencing*. Sistem ini akan memicu penguncian secara otomatis apabila mendeteksi penghuni yang meninggalkan area dalam radius tertentu, berdasarkan data dari GPS *smartphone*. Perhitungan dilakukan dengan dua parameter utama, yaitu *latitude* dan *longitude* (contoh koordinat: Latitude 40.7128° N, Longitude 74.0060° W). Lokasi GPS penghuni akan dievaluasi untuk menentukan apakah mereka berada dalam area yang telah ditentukan, sehingga sistem dapat memicu penguncian kamar secara otomatis. Selain itu, sistem juga akan membuka kunci secara otomatis apabila koordinat pengguna terdeteksi berada dalam area radius

*geofencing* yang telah ditentukan. Dengan demikian, sistem ini bekerja secara dinamis dalam dua arah: penguncian saat penghuni keluar dari area dan pembukaan kunci saat penghuni kembali ke area.

Untuk pencegahan terhadap kemalingan, data pintu yang sudah terkunci bisa menjadi acuan untuk mengaktifkan pengecekan gerakan dan jarak pada depan pintu untuk mengidentifikasi perilaku di depan pintu menggunakan sensor PIR, sistem ini diintegrasikan dengan sirine apabila terjadi pemicu yaitu perilaku yang tidak diizinkan, dimana terjadi gerakan saat penguncian tetapi sistem tidak membaca koordinat pengguna di radius yang ditetapkan. Sistem ini dapat aktif apabila pengguna tidak berada di sekitar pintu.

pemilihan algoritma *geofencing* didasarkan karena cenderung lebih efisien terhadap penguncian otomatis jika dan hanya jika penghuni meninggalkan area kos, sehingga lebih efisien apabila penghuni tidak jauh dari posisi kamar. *geofencing* juga didukung oleh penggunaan GPS yang menjadi fitur utama pada smartphone yang merupakan salah satu barang yang selalu dibawa oleh seseorang bepergian.

Pencatatan rekapitulasi juga disediakan pada solusi ini dengan mengambil data dari inputan aktivitas penguncian pintu. Pencatatan aktivitas pintu juga dicatat dengan timestamp untuk dapat menjadi rekapitulasi yang berguna.

## 2. Solusi 2

“Sistem Identifikasi Perilaku Mengancam dengan Algoritma *Decision Tree* berbasis RFID Sebagai Kontrol Penguncian”

*Decision tree* adalah model yang membagi dataset menjadi subset berdasarkan nilai atribut, membentuk struktur pohon dengan node keputusan dan node daun. Struktur pohon dimulai dari node akar, bercabang ke node keputusan, dan berakhir di node daun yang tidak dapat dibagi lagi.[5]

Sistem ini menggunakan teknologi RFID (*Radio Frequency Identification*) untuk mengidentifikasi penghuni kos. Setiap penghuni diberi tag RFID khusus yang

berfungsi untuk membuka atau mengunci pintu secara otomatis ketika tag tersebut terdeteksi oleh sensor di depan pintu. Integrasi dengan sensor gerak atau jarak memungkinkan sistem untuk mendeteksi keberadaan objek di dekat pintu. Jika objek yang terdeteksi membawa tag RFID yang sesuai, pintu akan terbuka secara otomatis untuk memfasilitasi akses masuk.

Sebaliknya, jika objek yang terdeteksi tidak memiliki tag RFID, sistem akan memberikan notifikasi kepada penghuni melalui aplikasi dan mengaktifkan sirine jika objek berupa manusia tersebut tetap berada di area pintu dalam jangka waktu tertentu. penggunaan *decision tree* pada solusi ini dikarenakan struktur logis dalam Pengambilan Keputusan dengan membagi data input menjadi cabang-cabang berdasarkan aturan tertentu yang logis. perilaku semacam ini dapat diklasifikasikan dengan berbagai parameter yang ada seperti objek yang terdeteksi di ketersediaan tag RFID, sensor gerak, dan durasi.

Jika objek tidak memiliki RFID, tetapi sensor tetap mendeteksi pergerakan, sistem akan memberikan respons berbeda berdasarkan durasi objek berada di sekitar pintu:

1. Durasi 10 Detik ( $t = 10s$ ):

Ketika objek terdeteksi berada dalam area pembacaan sensor selama 10 detik, sistem akan memberikan peringatan awal melalui notifikasi kepada pengguna. Notifikasi ini berisi informasi bahwa ada objek atau individu di sekitar pintu dan sistem akan memberi peringatan suara agar objek meminta pengguna untuk segera memberikan konfirmasi atau menghubungi penghuni terkait kedatangan tersebut.

2. Durasi 1 Menit ( $t = 60s$ ):

Jika objek tetap berada dalam area pembacaan sensor selama 1 menit, sistem akan memberikan peringatan tegas untuk segera menjauhi area pintu. Hal ini bertujuan untuk memperingatkan objek bahwa keberadaannya sudah memberikan tindakan ancaman dan diminta untuk meninggalkan lokasi.

### 3. Durasi 2 Menit ( $t = 120s$ ):

Jika objek tetap berada dalam area pembacaan sensor selama 2 menit tanpa menjauh, sistem akan mengeluarkan peringatan yang lebih serius. Peringatan ini meminta objek untuk segera menjauhi area pintu, dan sistem akan mengirimkan notifikasi lanjutan kepada pengguna untuk meningkatkan kewaspadaan dan memberikan langkah keamanan tambahan.

Sistem ini dirancang untuk meningkatkan keamanan dengan memantau pergerakan secara aktif dan memberikan peringatan sesuai dengan durasi deteksi objek di area sensor. Sistem ini menyediakan rekapitulasi sistem aktivitas penguncian pintu dengan melakukan pencatatan pada data waktu kunci saat terbuka dan tertutup. Data ini didapatkan dari output sistem yang digunakan.

### 3. Solusi 3

“Sistem Keamanan Dengan Melakukan Deteksi Pembobolan serta Pengenalan Wajah berbasis *Single Board Computer*”

*Convolutional neural network* (CNN) adalah arsitektur *deep learning* yang sering digunakan untuk mengatasi masalah klasifikasi gambar yang dirancang khusus untuk menangani tugas-tugas terkait pengolahan citra, seperti klasifikasi gambar, deteksi objek, dan pengenalan pola[6]. Metode yang digunakan ini membutuhkan *single board computer* untuk dapat melakukan pengolahan dari citra gambar yang diambil oleh kamera. Kamera berfungsi sebagai sensor visual yang terus memantau pergerakan dan aktivitas yang terjadi di area tersebut. Gambar atau video yang diambil oleh webcam kemudian diproses menggunakan model CNN untuk mengenali objek atau wajah.

Sistem keamanan yang dirancang memanfaatkan teknologi *deep learning* dan deteksi gerakan untuk mengidentifikasi identitas penghuni serta wajah yang tidak dikenal secara real-time. Sistem ini bekerja dengan mendeteksi gerakan menggunakan sensor dan menangkap citra dari kamera, yang kemudian diproses melalui algoritma

Haar Cascade untuk mendeteksi area wajah. Metode Haar Cascade digunakan untuk mengidentifikasi pola-pola spesifik seperti mata, hidung, dan bibir sebagai langkah awal deteksi wajah sebelum melanjutkan ke proses pengenalan identitas[7].

Setelah area wajah terdeteksi, sistem melakukan identifikasi keaslian wajah untuk memastikan tidak terjadi pembobolan melalui metode *spoofing*. Metode *spoofing* merupakan teknik pemalsuan identitas wajah menggunakan media seperti foto, video, atau topeng. Deteksi terhadap metode ini sangat penting pada sistem yang menerapkan pengenalan wajah untuk memastikan validitas autentikasi.

Pengenalan wajah ada pada tahap akhir, bekerja untuk mengonversi wajah yang terdeteksi menjadi representasi vektor numerik (*embeddings*). Representasi ini dibandingkan dengan database wajah yang dikenal untuk memverifikasi identitas penghuni. Jika identitas tidak dikenali atau wajah tidak dapat teridentifikasi, sistem akan memberikan peringatan suara untuk mencegah potensi ancaman serta mengirim notifikasi *real-time* kepada pengguna melalui koneksi nirkabel. Proses ini dirancang agar bekerja secara efisien, memberikan respons cepat untuk pembukaan kunci otomatis, dan mendukung pengamanan berbasis pengenalan wajah di lingkungan pintu.

### **1.2.3. analisis solusi**

untuk mengetahui solusi mana yang terbaik maka kita perlu melakukan analisa terhadap solusi solusi yang telah diberikan. untuk metode analisa yang akan digunakan adalah metode *House of Quality* (HoQ). *House of Quality* atau yang biasa disingkat HoQ merupakan sebuah alat yang mendukung metode *Quality Function Development*. HoQ terdiri dari beberapa bagian yaitu *Customer Needs and Benefits*, *Planning Matrix*, *Technical Response*, *Relationship Matrix*, *Technical Correlations*, *Technical Matrix* [8]. Matriks HOQ ini adalah upaya untuk mengkonversikan *voice of customer* secara langsung terhadap karakteristik teknis atau spesifikasi teknis dari sebuah perencanaan yang dihasilkan.

Relationships:  
 ⊙ Strong= 5  
 ○ Fair= 3  
 △ Weak= 1

		Computing Performance	Automatisasi penguncian	Notifications Capability	Output alarm	Deteksi pergerakan	Metode komputasi		Solusi 1	Solusi 2	Solusi 3	Importance rating	Percent of importance(%)
		↑	↑	↑	↑	↑	↑						
Low power consumption	4	△	△	△	○	△			○	⊙	○	4	25
Low cost	3	△	△	△	○	△			⊙	○	○	3	18.75
Pencatatan aktivitas pintu	4	○	○			○	○		○	○	⊙	4	25
Waktu pengerjaan < 6 bulan	5		○	○		△	△		○	○	○	5	31.25
Importance Rating		19	34	22	21	24	17	137	3.38	3.63	3.63		
Percent of Importance(%)		13.8	24.8	16.06	15.3	17.5	12.4	100					
Solusi 1		○	⊙	⊙	○	○	⊙	4.1				7.48	3.74
Solusi 2		○	⊙	⊙	○	⊙	○	4.2				7.83	3.87
Solusi 3		⊙	⊙	⊙	○	⊙	⊙	4.7				8.33	4.17

Gambar 1.1. House of Quality

dapat dilihat pada gambar 1. diatas, dimana tabel HoQ didapatkan dari relasi antara fitur dasar dan tambahan serta relevan pada masing masing solusi.

pada fitur *computing performance* (pemrosesan data) memiliki hubungan yang bertolak belakang dengan *low power consumption* (konsumsi daya rendah) dikarenakan kebutuhan pemrosesan tersebut berkaitan dengan komponen mikrokontroler dan mikrokomputer yang akan digunakan, sedangkan alat dengan performa pemrosesan juga berbanding lurus dengan daya yang digunakan. begitu juga dengan *low cost* (biaya rendah) dikarenakan kemampuan pemrosesan data tersebut semakin tinggi juga berbanding lurus dengan harga dihabiskan sehingga bertolak belakang dengan *low cost*. Fitur otomatisasi penguncian ini berkaitan sebanding dengan waktu pengerjaan, dikarenakan sistem dirancang dengan otomatisasi

penguncian menjadi output utama dari sistem, dan tidak menjadi fitur kompleks. Fitur dasar 2 tersebut berkaitan cukup dengan fitur pencatatan aktivitas pintu, semakin tinggi performa yang dapat diberikan semakin baik kemampuan multitasking dalam mengerjakan pemrosesan dan melakukan pencatatan.

Pada *notification capability* (kemampuan notifikasi) memiliki hubungan berlawanan dengan *low power consumption* dikarenakan notifikasi memerlukan daya pada software dan hardware untuk mengoperasikan sistem. Fitur ini juga memiliki hubungan yang berlawanan dengan *low cost* dikarenakan perangkat komponen yang diperlukan juga mempengaruhi biaya yang dihabiskan. Sama seperti fitur otomatisasi penguncian, fitur ini berkaitan sebanding dengan waktu pengerjaan dikarenakan fitur ini juga merupakan output dari sistem, dan tidak menjadi fitur kompleks.

Pada fitur deteksi pergerakan, memiliki hubungan berlawanan dengan *low power consumption* dan *low cost* dikarenakan fitur ini memungkinkan untuk menggunakan komponen seperti sensor, kamera dan sebagainya yang cukup berpengaruh terhadap konsumsi daya dan biaya. waktu pengerjaan berlawanan dikarenakan fitur ini memiliki kerumitan dikarenakan melibatkan analisis data dan implementasi sensor, kamera dan lain lain yang membuat waktu pengerjaan bisa lebih lama dari waktu yang direncanakan. Fitur ini berelasi cukup dengan fitur tambahan pencatatan aktivitas dikarenakan deteksi gerakan menjadi input dalam pencatatan pintu tetapi ada beberapa kondisi gerakan yang normal dicatat oleh pencatatan pintu sehingga keterkaitan pada tingkat mencukupi.

pada fitur metode komputasi, memiliki hubungan sebanding dengan output alarm, dikarenakan ini merupakan sebuah fitur tambahan yang memiliki metode komputasi menggunakan algoritma pemecahan masalah dalam mengeluarkan outputnya yaitu alarm itu sendiri. Fitur ini memiliki hubungan berlawanan dengan waktu pengerjaan dikarenakan fitur ini memiliki kompleksitas terkait algoritma yang digunakan baik dari penguncian pintu, identifikasi perilaku dan lain lain. Oleh sebab itu, semakin kompleks metode komputasi yang digunakan, semakin besar

kemungkinan bahwa waktu pengerjaannya melebihi target waktu kurang dari 6 bulan. Semakin efisien metode komputasi, semakin efisien dalam melakukan multitasking dalam hal ini adalah fitur pencatatan aktivitas pintu.

#### **1.2.3.1 Analisis Usulan Solusi 1**

Setelah menganalisis usulan solusi menggunakan *House of Quality* (HoQ), solusi "sistem kunci pintar menggunakan teknik Geofencing sebagai kontrol penguncian" memperoleh nilai akumulasi sebesar 4,1. fitur utama pada solusi satu yang memiliki nilai *strong* adalah fitur otomatisasi penguncian, notification capability, dan fitur metode komputasi. Pada fitur otomatisasi penguncian serta notification capability bernilai *strong* dikarenakan 2 fitur utama ini merupakan fitur utama.

Solusi ini juga sangat relevan dengan otomatisasi penguncian, karena fokus utama solusi adalah pada otomatisasi penguncian yang bergantung pada lokasi geografis pengguna. Sistem ini bersifat dinamis, di mana ketika pintu dalam keadaan terbuka dan posisi geografis pengguna melewati batas pagar virtual (geofence), maka penguncian otomatis akan diaktifkan.

fitur metode komputasi memiliki nilai *strong*, algoritma geofencing yang diimplementasikan cukup fleksibel. Algoritma ini mempermudah pemrosesan dan perbandingan status penghuni berdasarkan lokasi geografis dengan batasan geofence yang telah ditetapkan sebelumnya. Fitur ini memiliki nilai yang lebih tinggi dibanding solusi 2 dikarenakan komputasi yang digunakan cukup fleksibel.

#### **1.2.3.2 Analisis Usulan Solusi 2**

Setelah menganalisis usulan solusi menggunakan *House of Quality* (HoQ), solusi "sistem identifikasi perilaku mengancam dengan algoritma Decision Tree berbasis RFID sebagai kontrol penguncian" memperoleh akumulasi nilai sebesar 4,2. fitur utama pada solusi dua yang memiliki nilai strong adalah fitur otomatisasi penguncian serta notification capability dikarenakan 2 fitur ini adalah fitur utama dari sistem seperti pada 2 solusi lainnya.

Solusi ini memiliki kaitan yang sebanding dengan *computing performance*, karena solusi ini membutuhkan komputasi yang lebih tinggi dibandingkan dengan solusi sebelumnya, meskipun masih dapat dijalankan menggunakan komponen seperti mikrokontroler. Data yang diproses berupa input sensor jarak, durasi, dan input RFID yang menunjukkan status penghuni.

Solusi ini juga terkait langsung dengan fitur deteksi pergerakan mengancam. Algoritma Decision Tree digunakan untuk menganalisis berbagai parameter, seperti apakah objek membawa tag RFID, durasi kehadiran di sekitar pintu, dan pergerakan yang terdeteksi. Berdasarkan analisis tersebut, sistem dapat mengklasifikasikan apakah objek yang terdeteksi bertindak normal atau melakukan tindakan yang tidak diizinkan.

Terakhir, solusi ini juga berkaitan dengan fitur metode komputasi. Algoritma Decision Tree yang digunakan dalam solusi ini memungkinkan sistem untuk mengidentifikasi perilaku mengancam berdasarkan input yang tersedia. Namun, penguncian otomatis tidak bergantung pada algoritma yang kompleks, melainkan dipicu oleh status penghuni yang sudah terdeteksi melalui RFID..

### **1.2.3.3 Analisis Usulan Solusi 3**

Setelah menganalisis usulan solusi menggunakan *House of Quality* (HoQ), solusi "sistem keamanan dengan melakukan deteksi pembobolan serta pengenalan wajah berbasis single board computer" memperoleh akumulasi nilai sebesar 4,7. fitur utama pada solusi dua yang memiliki nilai strong adalah fitur otomatisasi penguncian

serta notification capability dikarenakan 2 fitur ini adalah fitur utama dari sistem seperti pada 2 solusi lainnya.

Solusi ini sangat terkait dengan *computing performance* karena pemrosesan visual yang digunakan dalam mengenali wajah membutuhkan daya komputasi tinggi. Algoritma yang digunakan dalam proses pengenalan wajah, seperti Haar Cascade dan FaceNet, memerlukan pemrosesan gambar yang cukup intensif, namun mampu memberikan hasil yang lebih akurat dalam mendeteksi perilaku yang tidak diizinkan.

Pada fitur deteksi pergerakan, solusi ini memiliki keunggulan karena algoritma *face recognition* dapat membedakan antara penghuni dan orang asing, serta mendeteksi aksi pembobolan yang dilakukan melalui metode *spoofing*. Keberadaan kamera memungkinkan sistem mengidentifikasi perbedaan antara individu yang memiliki hak akses dan yang tidak, sehingga dapat memberikan respons yang sesuai. Dengan demikian, sistem dapat menilai apakah suatu perilaku termasuk diizinkan atau tidak.

Untuk metode komputasi, solusi ini menggunakan algoritma berbasis deep learning, seperti Haar Cascade dan FaceNet, yang lebih kompleks dibandingkan solusi lainnya. Meskipun memerlukan pengolahan gambar yang intensif, solusi ini tetap memberikan hasil yang lebih akurat dalam mengetahui pergerakan tidak sah. Selain itu, sifat biometrik dari sistem face recognition memastikan bahwa objek tidak dapat memalsukan fungsi sistem, karena pengenalan wajah merupakan sistem otentikasi yang unik dan tidak dapat dipalsukan.

#### **1.2.4. Solusi yang Dipilih**

Dalam evaluasi berdasarkan fitur dasar, solusi ketiga, yaitu *sistem keamanan dengan deteksi pembobolan dan pengenalan wajah berbasis single-board computer*, dinilai unggul dibandingkan dua solusi lainnya. Solusi ini dianggap terbaik karena memiliki akurasi deteksi pembobolan yang tinggi, yang merupakan prioritas utama dari sistem yang akan dikembangkan. Sistem ini mampu mengenali pengguna tanpa

memerlukan peralatan tambahan seperti tag RFID atau perangkat dengan modul GPS, sehingga lebih praktis bagi pengguna. Selain itu, sistem ini menawarkan fleksibilitas dalam mendeteksi pergerakan tidak diizinkan, sedangkan dua metode sebelumnya memiliki kelemahan dalam mengenali objek sebagai pengguna tanpa memastikan identitas sebenarnya.

